The PDP Bill 2019 Through the Lens of Privacy by Design

12th November, 2020

By **Saumyaa Naidu, Akash Sheshadri, Shweta Mohandas,** and **Pranav M Bidare**

Edited by **Arindrajit Basu** and **Shweta Reddy**

With inputs from **Amber Sinha**

Visualisation Designed by **Akash Sheshadri**

The Centre for Internet and Society, India

Shared under
Creative Commons Attribution 4.0 International license

Background

The Personal Data Protection (PDP) Bill, 2019 was introduced in the Lok Sabha on December 11, 2019 by the Minister of Electronics and Information Technology. The Bill aims to provide for protection of personal data of individuals, and establishes a Data Protection Authority for the same[1]. The PDP Bill, 2019 contains several clauses that have implications on the visual design of digital products. These include the specific requirements for communication of notice and consent at various stages of the product. The Bill also introduces the Privacy by Design policy. Privacy by Design (PbD), as a concept, was proposed by Ann Cavoukian in the 1990s, with the purpose of approaching privacy from a design-thinking perspective[2]. She describes this perspective to be holistic, interdisciplinary, integrative, and innovative. The approach suggests that privacy must be incorporated into networked data systems and technologies, by default[3]. It challenges the practice of enhancing privacy as an afterthought. It expects privacy to be a default setting, and a proactive (not reactive) measure that would be embedded into a design in its initial stage and throughout the life cycle of the product[4]. While PbD is a conceptual framework, it's application can change the way digital platforms are created and the way in which people interact with them. From devising a business model, to making technological decisions, PbD principles can make privacy integral to the processes and standards of a digital platform.

The PDP Bill states that data fiduciaries are required to prepare a Privacy by Design policy and have it certified by the Data Protection Authority. According to the Bill, the policy would contain the managerial, organisational, business practices and technical systems designed to anticipate, identify and avoid harm to the data principal[5]. It would mention if the technology used in the processing of personal data is in accordance with the certified standards. It would also comprise of the ways in which privacy is being protected throughout the stages of processing of personal data, and that the interest of the individual is accounted for in each of these stages. Once certified by the Data Protection Authority, the data fiduciaries are also required to publish this policy on their website[6]. This forces the data fiduciaries to envision privacy as a fundamental requirement and not an afterthought. Such a policy would have a huge impact in the way digital platforms are conceptualised, both from the technological and the design point of view. The adoption of this policy by digital platforms would enable people to know if their privacy is protected by the companies, and what are the various steps

[1] https://prsindia.org/billtrack/personal-data-protection-bill-2019

[2] https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

[3] https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

[4] https://www.smashingmagazine.com/2019/04/privacy-ux-aware-design-framework/

[5] http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

[6] https://sflc.in/key-changes-personal-data-protection-bill-2019-srikrishna-committee-draft

being taken for this purpose. Besides the explicit Privacy by Design policy, the PDP Bill, 2019, also recommends the regulations for data minimisation, establishment of the Data Protection Authority (DPA), and the development of a consent framework. These steps are also part of the Privacy by Design approach.

This paper evaluates the PDP Bill based on the Privacy by Design approach. The Bill's scope includes both the conceptual and technological aspects of a digital platform, as well as the interface aspect that the individual using the platform faces. The paper will hence analyse how PbD approach is reflected in both these aspects. At the conceptual level, it will look at the data ecosystem that the Bill unwittingly creates, and at the interface level, it will critically analyse the Bill's implication on the notice and consent communication in the digital products. This includes the several points of communication or touchpoints between a company and an individual using their service, as dictated by the Bill, and how they would translate into visual design. Visual design forms an integral part of digital platforms. It is the way in which the platforms interact with the individuals. The choices made by individuals are largely driven by the visual structuring and presentation of information on these platforms. Presently, the interface design in several platforms is being used to perpetuate unethical data practices in the form of dark patterns. Dark Patterns are deceptive user interface interactions, designed to mislead or trick users to make them do something they don't want to do[7]. The design of the notice and consent touchpoints can significantly influence the enforcement of this Bill, and how it benefits individuals. Moreover, digital platforms may technically follow the regulations but can still be manipulative through their interface design. Thus, the role and accountability of design becomes crucial in the interpretation of the data protection regulations.

PDP Bill 2018 vs 2019 from a Design Perspective

The most recent draft of the Personal Data Protection Bill, 2019 has been in the public domain since December, 2019. However, an earlier version of the draft bill was released in 2018, and since then received comments, feedback, and critique at various stages. Some key differences between the 2018 version of the bill, and the 2019 version range from small differences to important definitions such as personal data, and sensitive personal data, to broader systemic changes such as the regulation of the transfer and storage of personal data outside the country.

Interesting differences between the drafts from the PbD approach include the changed rights of a data principal, the introduction of social media intermediaries, and the section on "Privacy by Design." In the 2018 draft, the data principal possessed specific rights with

[7] https://uxdesign.cc/dark-patterns-in-ux-design-7009a83b233c

respect to their personal data, which included the right to obtain confirmation on the processing status of the data, seeking correction or transfer of data, and restricting the continuous disclosure of data. The 2019 draft retains these rights, but also introduces to data principals, the additional right of erasure of personal data, which is no longer essential for the original purpose of collection and processing. This added right brings with it a necessary reimagining of the way in which data management systems are to be designed on digital platforms. The PbD principles also mention secure lifecycle management of information, and that personal information should be retained only as long as necessary to fulfill the stated purposes, and then securely destroyed[8].

Social Media Intermediaries (SMIs) are another newly introduced concept in the 2019 Bill. SMIs are a type of data fiduciary, and they are defined as intermediaries which facilitate online interaction between users, allowing for the sharing of information. This definition clearly encompasses entities that offer social media services such as Facebook and Twitter, but is broad enough to also include those that offer messaging services, like Whatsapp, Signal, and Telegram. The bill however specifically excludes e-commerce entities, internet service providers, search engines, and email services. While the definition may seem broad, it is important to distinguish SMIs because of additional necessary obligations that may be imposed on them. All SMIs which have a user base size above/beyond a predetermined threshold qualify as ”significant” data fiduciaries, and the actions of these users are considered to be capable of impacting electoral democracy or public order in the country. All “significant” SMIs must provide a voluntary user verification mechanism for all users in India. This addition adds accountability for the SMIs, and also implies changes in the design of social media platforms.

The 2018 draft Bill did include the obligation for all data fiduciaries to publish a “Privacy by Design” policy. While the 2018 draft did not specify any obligation connected to the standards for this policy, the 2019 draft gives every data fiduciary the option to have their Privacy by Design policy audited and certified by the Data Protection Authority of India (DPAI). Once this certificate is obtained, it must be published on the websites of both the data fiduciary, and the DPAI. This certificate however is required for a fiduciary to be eligible to apply for inclusion in the Innovation Sandboxes proposed to be set up by the DPAI. The introduction of and specifications under the Privacy by Design policy are a direct adaptation of the PbD approach asking data fiduciaries to apply the principles of PbD in all aspects of their development and infrastructure.

[8] https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

Understanding the Data Protection Ecosystem

The PDP Bill 2019 envisages a data protection regime through an ecosystem of entities, and proceeds to establish their relationships, roles, and responsibilities. The roles and relationships of these entities are limited by their definitions as presented in the Bill. In case of more complicated ecosystems, there is the question of interchangeability of these roles, and hence their identities may or may not be apparent to the data principal. The onus of clearly communicating these identities rests with the data fiduciary, through effectively designed privacy policies. On further scrutiny, it can be argued that the ecosystem thus created, could be traditionally hierarchical, which tends to exclude the data principal and work conversely to their interest. It is thus, useful to emulate the principles of PbD and systems thinking[9] by imagining a data principal-centered ecosystem, that can be conveyed to a general audience.

It has been observed that at the intersection of different entities emerge certain information touchpoints, that are driven-by and that document their actions. For example, a privacy notice can be imagined as a fundamental touchpoint of the ecosystem that informs a data principal of a data fiduciary's practices with regard to their data. Similarly, consent mechanisms like forms are touchpoints that affirm/attest the usage of their data. A data trust score sheet on the other hand can be seen as a touchpoint that emerges between an auditor and the Data Protection Authority. It is upon the data fiduciary to communicate the data trust score sheet to the data principal[10]. Data fiduciaries are expected to leverage digital experiences to communicate such touchpoints in the form of well designed notices.

Digital experiences should be designed to communicate touchpoints to the data principal that are otherwise communicated without their knowledge. Understanding the data protection ecosystem through these touchpoints can help align practices towards better transparency and increased accountability of data fiduciaries, with regard to the data of its subjects. Best practices that surround the design space of privacy notices can be extrapolated to design these touchpoints. Touchpoints, like notices, can be understood to manifest differently as a part of any digital experience. Notices could be passive as a policy, terms of service/conditions, or active where data principals could exercise their consent when presented as forms/confirmation dialogs. They could be served in-context of the service, in addition to being referred to, before a principal signs-up for the same. The Bill does little to highlight the multimodality of touchpoints.

---

[9] https://medium.com/disruptive-design/tools-for-systems-thinkers-the-6-fundamental-concepts-of-systems-thinking-379cdac3dc6a

[10] The Personal Data Protection Bill, 2019, 373 of 2019, Cl. 7. http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

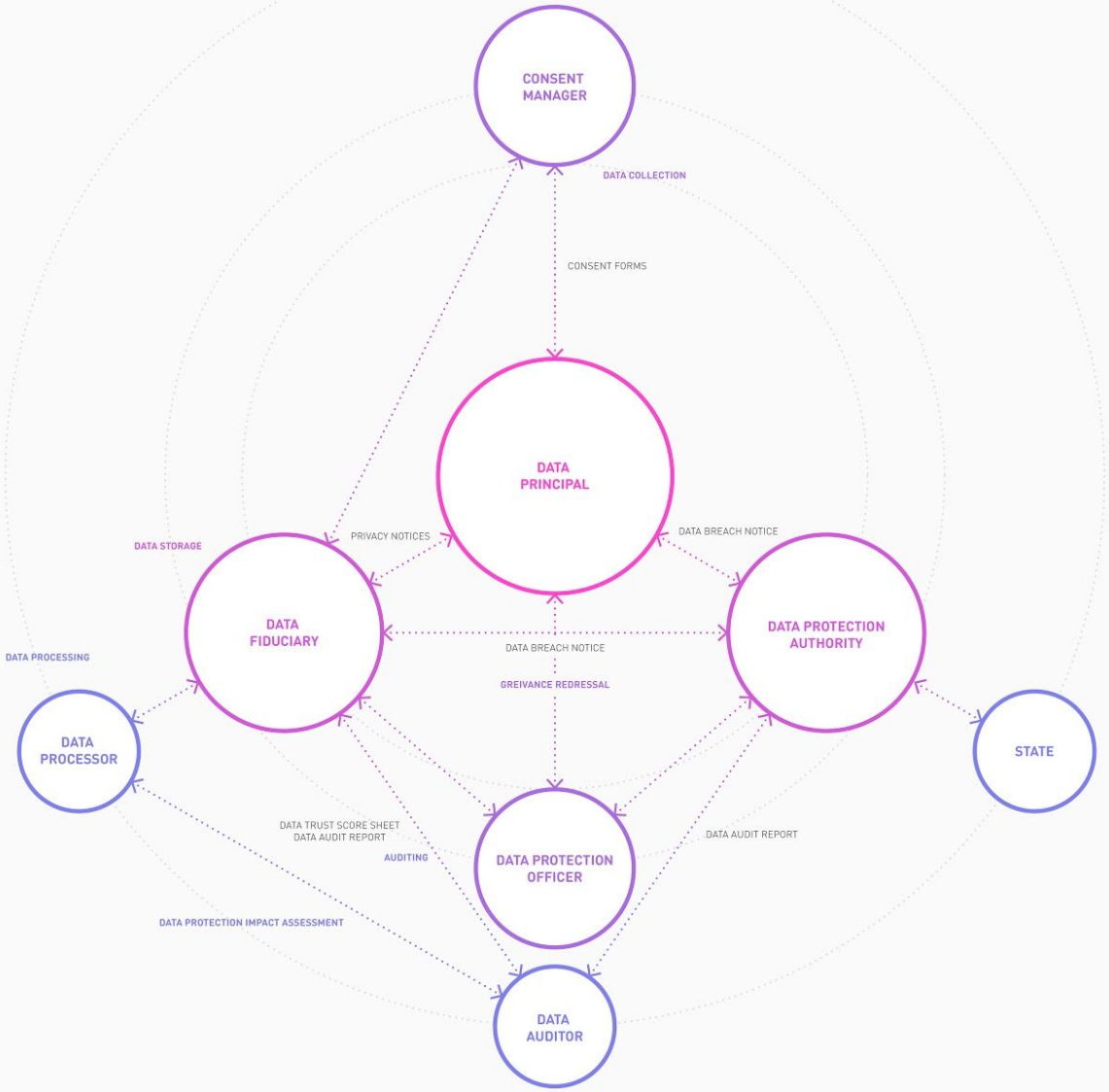
Notices should communicate the ecosystem in the context of a service, thereby highlighting channels for redressal for a data principal. The idea of notices should be transposed to universalise communication between all entities of the ecosystem. For instance, the principal could receive an alert of data being shared, breached, etc. simultaneously while the Authority is notified. A unified digital environment like consent aggregators could provide for the means of approving, altering, and revoking consent through nested channels amongst actors.

The emphasis on the demand for privacy as a service[11] has grown, so much so, that services are reaching out to their customers with data protection as a feature. The scope of the Bill should be widened to recognise privacy as a service and move beyond merely notice and consent communications. An interesting example as observed in the context of the ecosystem, is how an auditor assigns a rating in the form of a data trust score to the data fiduciary as a result of a data audit. Presently, the data fiduciary can choose to share it with the data principal. However, it should be made mandatory for the data fiduciary to make this rating available to the data principal before they subscribe to the services in question. Users tend to ascribe the ratings of services on digital platforms like an app store to judge the quality of services they provide. Digital experiences can, through a rating mechanism, leverage privacy respecting/enhancing fiduciaries over their counterparts. This rating can hence inspire accountability amongst data fiduciaries.

[11] https://360.here.com/the-next-wave-of-privacy-could-be-privacy-as-a-service

Data Protection Ecosystem

Entities & Touchpoints



The data protection ecosystem as explained in the Bill could be understood through the interactions between three main entities: data principal, data fiduciary and the Data Protection Authority. The ecosystem here is visualised to emphasize a data principal-centered model, with the perceived relevance of each entity corresponding to their size and their relative distance (radial hierarchy) to the data principal. Emerging touchpoints are mapped at the exchanges of these entities. For instance, consent forms could be more relevant to the data principal in comparison to a rather less actionable data audit report. This helps to understand user-facing touchpoints and how they can be communicated better to the data principal. Touchpoints also vary according to the purpose like data collection, storage, auditing, etc. as shown in the diagram in color.

As seen in this section, the notice and consent mechanisms carry a large part of the weight in terms of giving the data principal more control, hence abiding by the PbD principle of empowering the individuals[12]. The design of these mechanisms thus, are critical in the application of the PbD approach. It becomes important to understand the existing notice and consent mechanisms and how they can be improved upon from a design point of view.

Notice and Consent Communication

The existing notice and consent privacy approach has been criticised for placing the onus of privacy protection on the individual[13]. The notices present information on the data practices in a cryptic and tedious way, making it difficult for the individual to access and comprehend it. It becomes the responsibility of the individual to read and understand the notices before consenting to the data practices. In practice, privacy notices are rarely read by individuals. The lengthy textual notices with complex language make it impractical for people to go through it. This is also owing to the difficulty faced by individuals in making meaningful decisions for their privacy preferences. Short-term benefits are often chosen over long-term privacy even in instances when the implications are communicated[14]. In many other instances, the choice is false and users cannot opt-out of giving up their privacy. The use of several digital platforms is conditional upon consenting to the notices. Even if they do not wish to consent to the data practices of a digital platform, they do not have the choice to do so. Thus, in practice, these notices are considered to be merely an informational statement rather than an interactive control panel[15].

---

[12] https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

[13] https://www.jstor.org/stable/pdf/10.5325/jinfopoli.9.2019.0037.pdf?refreqid=excelsior%3A1fe3402f69f87147b62d28ccac482c4a

[14] https://arxiv.org/pdf/2001.02479.pdf

[15] https://arxiv.org/pdf/2001.02479.pdf

In order to create more effective privacy notices, several frameworks have been proposed; Privacy by Design, privacy impact assessments, audience oriented notices, layered notices, notices with relevant and actionable information, and usability evaluation[16]. Before delving into the PDP Bill and its recommendations on notice and consent mechanisms, it is necessary to look into how other regulations have dealt with it.

Notice and Consent Design Response After GDPR

The General Data Protection Regulation (GDPR) is the primary law regulating how companies protect EU residents' personal data. It applies to each member state of the European Union, aiming to create more consistent protection of consumer and personal data across EU nations[17]. Since the enforcement of the GDPR[18] in May 2018, design guidelines proposing privacy considerations that are in compliance with the GDPR have been set forth by several designers. The GDPR makes Privacy by Design a legal requirement[19]. Various sets of user experience (UX) guidelines have come up for designers to implement the PbD approach on digital platforms. UX design involves the entire process of acquiring and integrating a product, including aspects of branding, design, usability and function[20]. In order to ensure privacy on digital platforms, all these aspects are needed to be rethought. These UX guidelines primarily apply to notice and consent communication in digital platforms.

Privacy notices are one of the key notice and consent mechanisms. It should be noted that privacy notices are separate from the general terms and conditions[21]. Privacy notices are specific to information related to privacy of the individuals. Based on the PbD principles, the following design guidelines are suggested for the design of effective notices:

- **Timing -** Notices can be issued during on-boarding, registering an account, displaying privacy policy, and in-app consent. Several design guidelines speak about the just-in-time notices[22]. These are notices that are given at the time of collection of data. This could be through forms, or during a change in the settings. Just-in-time notices allow the advantage of informing an individual of the data they will share as they perform an action.

---

[16] https://www.ftc.gov/system/files/documents/public_comments/2015/10/00038-97832.pdf

[17] https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection

[18] https://gdpr-info.eu/

[19] https://www.secretstache.com/blog/integrating-privacy-by-design/

[20] https://www.interaction-design.org/literature/topics/ux-design

[21] https://uxdesign.cc/what-does-gdpr-mean-for-ux-9b5ecbc51a43

[22] https://www.secretstache.com/blog/integrating-privacy-by-design/

- **Volunteered and Automated Data Collection -** For designing clear privacy and data sharing notices, two ways of personal data collection have been identified; volunteered and automated[23]. While volunteered data collection is when an individual shares data through forms, etc., automated data collection happens through cookies, tracking scripts and other applications that are being used by the platform. Volunteered personal data collection notice should cover all potential ways in which the data can be used, and include a description of data storage. For automated personal data collection, user interface (UI) elements for information, and option to accept or refuse use of cookies should be used[24], besides providing details of data use and storage.

- **Updates on Breaches and Changes -** Communication strategies should be set up in case of a breach. Changes in the privacy policies should be summarised in a user-friendly way[25].

For consent mechanisms, the following guidelines have been suggested:

- **Granular Consent -** Granular consent for all data processing activities should be taken.

- **Right to Withdraw Consent -** Individuals should have the right to withdraw consent at any time.

- **Default Options -** The default settings of digital platforms should not contain any pre-checked boxes in the options[26].

- **Consent Management Platforms -** In order to conform with the GDPR's requirement around consent during collection and processing of personal data, consent management platforms (CMP) were introduced. A consent management platform (CMP) enables companies to automate their consent management process[27]. It informs individuals about the types of data being collected and what it will be used for. CMPs store individual consent data and handle requests to make alterations about the data the website has collected about them, including requests to access and erase this data. The design of these CMPs affect the consent choices of users.

---

[23] https://www.secretstache.com/blog/integrating-privacy-by-design/

[24] https://www.secretstache.com/blog/integrating-privacy-by-design/

[25] https://www.smashingmagazine.com/2019/04/privacy-ux-aware-design-framework/

[26] https://www.deptagency.com/story/gdpr-update-implicit-consent-and-pre-check-boxes-forbidden/

[27] https://www.cmswire.com/information-management/what-is-a-consent-management-platform/

A recent empirical survey of consent management platforms (CMP) conducted, indicates the use of dark patterns in digital platforms even after GDPR[28]. On studying the design of popular CMPs, it was found that dark patterns are still prominent in the platforms. The study looking at the legal quality of consent, concluded that implicit consent is more common on websites, most CMPs make rejecting all tracking substantially more difficult than accepting it, and while attempting to amend the consent settings, pre-ticked boxes are encountered[29]. Following a field experiment to investigate the impact of some of the most common designs on consent choices, it was found that notification style (banner or barrier) has no effect; removing the opt-out button from the first page increases the probability of consent; and providing more granular controls on the first page decreases the probability of consent[30]. These observations lead to the inference that even when there is legal compliance with the GDPR, digital products still find a way to take consent through unethical means. The study suggests using more detailed and durable ways of setting privacy preferences, potentially within the browsers. It also mentions that designers can play a role in creating tools for the regulators, and not just for users or websites[31].

Another approach suggested by Daniel Susser, speaks of decoupling 'notice' and 'consent', and looking at the independent benefits of 'notice'[32]. As notice and consent as a whole, has been criticized for failing to facilitate individual agency over data, notice alone can be approached as a privacy disclosure mechanism. This can lead to increased transparency of data collection, storage, and sharing systems[33]. Susser mentions that in the notice and consent framework, notice has the function of informing the user of the data practices based on which they can make a decision about their privacy preferences. In this scenario, without consent, notice has no function. Susser argues that notice could fulfill other functions such as providing basic situational awareness on data collection and processing, equipping users with the information needed to protect their privacy through nonlegal means, and alerting them to the fact that they need to assert other rights. Additionally, notice can play an

[28] https://arxiv.org/pdf/2001.02479.pdf

[29] https://arxiv.org/pdf/2001.02479.pdf

[30] https://arxiv.org/pdf/2001.02479.pdf

[31] https://arxiv.org/pdf/2001.02479.pdf

[32] https://www.jstor.org/stable/pdf/10.5325/jinfopoli.9.2019.0037.pdf?refreqid=excelsior%3A1fe3402f69f87147b62d28ccac482c4a

[33] https://www.jstor.org/stable/pdf/10.5325/jinfopoli.9.2019.0037.pdf?refreqid=excelsior%3A1fe3402f69f87147b62d28ccac482c4a

indirect role in supporting user interests through empowering third parties that advocate on behalf of users, and by encouraging good corporate behavior[34].

Alternatively, in order to preserve individual choice and focus on improving the known issues with privacy decision-making, another approach highlights designing for reflection. This approach supports the privacy self management model. It argues that designers of technological artefacts are responsible for triggering and guiding reflection amongst individuals interacting with their products and services[35]. It highlights three design guidelines: "friction, which serves as a trigger for further reflective thinking as well as an invitation for individuals to consider alternative values, beliefs, and assumptions; reflection, which allows individuals to better understand how artefacts influence the values, beliefs, and assumptions of themselves and others; and, controls, which is not only required by reflection to have an effect, but also increases the fairness of notice and consent"[36].

Besides notice and consent, some other UX design choices can also help in compliance with the PbD principles, and thereby the GDPR.

- **Easy Access to Data Settings -** Instead of complex routes to closure or deletion of accounts, the interface should allow for easy access to closing or deleting an account.

- **Data Minimisation, and Optimisation for Export or Deletion -** Another critical principle of PbD is data minimisation. It suggests that the identifiability and linkability of the personal data collected should be kept to a minimum[37]. This can be done through data pseudonymization, which involves replacing the personally identifiable data with an anonymous ID, token, or pseudonym. Further, PbD also states that whenever personal data is collected, it is structured in a way that is optimised for export and deletion at a later point[38].

- **Privacy Impact Assessment -** The design recommendations include privacy impact assessment (PIA), which is a process of documenting the issues, questions, and actions required to implement a healthy PbD process in a project, service, or product. PIAs are again a core requirement of GDPR[39].

---

[34] https://www.jstor.org/stable/pdf/10.5325/jinfopoli.9.2019.0037.pdf?refreqid=excelsior%3A1fe3402f69f87147b62d28ccac482c4a

[35] https://firstmonday.org/ojs/index.php/fm/article/view/9358/8051#p4

[36] https://firstmonday.org/ojs/index.php/fm/article/view/9358/8051#p4

[37] https://www.secretstache.com/blog/integrating-privacy-by-design/

[38] https://www.smashingmagazine.com/2019/04/privacy-ux-aware-design-framework/

[39] https://www.smashingmagazine.com/2017/07/privacy-by-design-framework/

Notice and Consent Design in the Context of PDP Bill 2019

The Bill recommends several communication points between the data fiduciary and the data principal. The design of platforms would be required to implement these recommendations. This section uncovers how these platforms need to accommodate the different types of notices and consent mechanisms from an interface design perspective, when they follow the Bill's recommendations.

Privacy Notices

The Bill asks for several details to be shared when personal data is being collected. The privacy notice hence would include the purpose of collection, nature and categories of personal data being collected, the identity and contact details of the data fiduciary, and contact details of the data protection officer (if applicable), right to withdraw consent and the procedure for this, consequences of failure to provide data, source of collection if not the data principal, entities the data will be shared with, any cross border transfer related information, period for which data will be retained, procedure for exercising right to access and confirmation, procedure for grievance redressal, right to file complaints, and data trust score (if applicable). In order to provide clear information both in the privacy notice and at the time of collection of personal data, the notifications to the data principal can be categorised under on-boarding and just-in-time notices.

- **On-Boarding Notices -** The on-boarding notice would be the same as the privacy notice which would be shown to the data principal as they register on the platform. This would also be available for them to view at all times on the platform. In order to accommodate the information clearly so it can be comprehended by the data principal, the notice can be designed to have clear sections, easy navigation, visuals, and interactive elements. Layering of information as a way of displaying privacy and data sharing notices should be practiced in the design of privacy notices so that the data principal can access it easily. This can be done through using summaries, visuals, and specific sections. The on-boarding or privacy notice will be required to communicate several other details. It should have a separate section on the right to access identities of data fiduciaries in one place, along with categories of personal data shared with them.

- **Just-in-Time Notices** - The just-in-time notice would include the information that the Bill asks the data fiduciary to notify at the time of collection of personal data. This would include specific purpose of collection, nature and categories of data, consequences of failure to provide such data, source of collection (if not the data principal), and the entities the data will be shared with. These can be shown using just-in-time notices in the form of pop-up boxes as the data principal interacts with the platform and performs any activity that requires personal data collection.

Periodic Notifications

The Bill requires the data fiduciary to notify individual data principals at different stages of the use of a platform, and about important operations on the processing of personal data. For example, notifications are to be sent to individuals in case the personal data process is incomplete, inaccurate, misleading and not updated, when it is shared with other entities. Thus, periodic notifications can be given during the interaction with the platforms and in the form of clear, visual emails/notifications. This category of notification also includes confirmation of whether personal data is being processed or has been processed, personal data (or summary), and summary of processing activities, according to the right to confirmation and access. Where processing has been carried out by automated means, the data principal has the right to receive personal data in a structured, commonly used, machine-readable format. This should be notified as well to individual data principals via an email or platform notification.

Breach Notifications

In case of breach of personal data, the Bill dictates that a notice to inform the Data Protection Authority should be sent. The Authority shall then determine if the data principal is to be notified by the data fiduciary. This notification to the data principal must be visually segregated, plain language explanation of the breach. The consequence of the breach and further steps should also be given to the data principal. It should inform them of the nature of the personal data that has been breached and the number of data principals affected. This notice should be sent to individuals through email/notification as well as displayed on the website.

Access to Notices on Websites

With a large amount of information to be conveyed through privacy notices, IoT devices such as smart watches, or even smartphones face the challenge of not being able to display the notices as clearly due to limited screen space. The notices in these devices can be designed to have critical information along with prompts that direct the data principal to the website for a longer version of the notice. Several details are also meant to be communicated through the website in a way that the data principal can find their way to it easily. This leads to the need for specific guidelines that dictate how the website should be designed to display privacy related information.

Obtaining Consent

The Bill calls for free, informed, specific, clear, consent which is capable of being withdrawn. It also recommends giving or withdrawal of consent through a consent manager. In order to achieve this, granular controls while selecting consent choices would help individuals make

informed and specific decisions. Easy access to data settings should be provided. The interface of the platforms should allow for simpler ways of rejecting tracking. There should be no pre-ticked boxes or default acceptance. The consequence of not allowing consent for a specific data collection should be given to the data principal. According to the Bill, consent for sensitive personal data must be explicitly obtained by stating the purpose or operation likely to cause significant harm in clear terms, along with the choice of separately consenting to the purposes and operations. Thus, consent for sensitive personal data need to be sought separately clarifying what it comprises.

Indian Languages, Plain Language, and Accessibility in Notices

The scope of PbD also extends details such as designing privacy experiences for the vulnerable users such as children, elderly, and persons with disabilities[40]. Accessibility considerations such as the policies being screen reader compatible and available in multiple languages also add to the PbD approach. This section examines the existing scenario of languages and accessibility in further detail.

Privacy policies help inform the user or potential user about the data collection practices and serve as a basis for user browsing and transaction decisions[41]. More specifically, privacy policies lay out what data is collected, the purpose of the collection and use, whether the data is shared with other entities, and how long the data will be retained[42]. However, in order to understand these conditions the user must be able to read the privacy policy. The Sensitive Personal Data or Information (SPDI) Rules of the IT Act require that the privacy policy be "comprehensible and easy to understand by a non legal person". Additionally, both the 2018 and 2019 versions of the PDP Bill specify the need for the privacy policies to be in such a manner that they are "concise… easily comprehensible to a reasonable person and in multiple languages where necessary and practicable".

Although, there seems to be legal requirements in place to ensure the easy readability of the privacy policies, the framing, format and structure of the policies are decided by the companies. A study of forty privacy policies of financial companies in the United States of America revealed that some of the policies required an equivalent of post graduate education to understand it. The other policies required a minimum of twelve years of schooling to understand[43]. In India, a study of privacy policies of Indian service providers revealed that the service providers in their privacy policies used vague and undefined

[40] https://www.smashingmagazine.com/2019/04/privacy-ux-aware-design-framework/

[41] https://ssl.lu.usi.ch/entityws/Allegati/pdf_pub1430.pdf

[42] A Privacy Policy Model for Enterprises

[43] https://ssl.lu.usi.ch/entityws/Allegati/pdf_pub1430.pdf

terminologies[44]. Similarly, another study of forty eight Fintech companies in India revealed that only twenty privacy policies were easy to understand[45]. However, the concern does not end with the legalese, in a country like India with both low literacy and multiple languages spoken. While the number of mobile phone users are growing and the number of people using apps are increasing day by day most of the notices are still in English, or in formats which are not screen reader compatible. For example, the above mentioned study of privacy policies of Fintech companies revealed that out of the forty eight companies (most of which are used by a large number of people) only two companies had privacy policies in an Indian language[46].

Even with regard to screen reader capability, a number of privacy policies are still incompatible with screen readers, preventing yet another group of people from giving informed consent[47]. Screen readers help individuals who find it impossible or difficult to read, have the information read out to them. A text-only version of a page with labels for images allows the usage of screen readers to access the information the same way as a sighted reader. A study of over seven thousand Indian government websites revealed that thirty three per cent of the websites have no alternate text available for the images[48]. The test also revealed that ninety five percent of the websites had anywhere between 1-500 errors with regard to HTML validation. The ignorance of HTML standards further creates inaccessibility on web browsers for individuals using screen readers[49]. While privacy policies are already difficult to read and comprehend, it is tough to expect more accessibility features when most websites are not screen reader compatible.

If it is believed that meaningful consent is only possible when the individual has read the entire notice, we need to make the notices as easily understandable to individuals with different levels of abilities. The idea of accessibility either through language, screen reader compatibility, voice or video explainers, would go a long way in fulfilling the notice and consent model.

---

44 https://cis-india.org/internet-governance/blog/a-study-of-the-privacy-policies-of-indian-service-providers-and-the-43a-rules

45 https://cis-india.org/internet-governance/files/Hewlett%20A%20study%20of%20FinTech%20companies%20and%20their%20privacy%20policies.pdf

46 *Ibid.*

47 https://www.wired.com/story/web-accessibility-blind-users-dominos/

48 https://cis-india.org/accessibility/accessibility-of-govt-websites.pdf/view

49 https://cis-india.org/accessibility/accessibility-of-govt-websites.pdf/view

Conclusion

While the PDP Bill 2019 follows the principles of PbD in essence, the design of the interfaces of the digital platforms, which the individuals eventually interact with, would influence whether it safeguards the privacy of individuals or not. In terms of the data ecosystem that is formed based on the Bill, the data principal should be at the centre, allowing them more control. In terms of the interface, clearer guidelines for the visual design of notice and consent mechanisms should be prescribed in the Bill.

Despite the detailed recommendations by the Bill regarding notice and consent, the use of dark patterns in design can influence the way in which information is seen and accessed by the data principal. As seen in the case of GDPR compliance, several design choices can lead to inaccessible notices, even as they technically follow the Bill's recommendations. The Bill doesn't directly address dark patterns but gives a vague direction towards using "clear, concise, and easily comprehensible" ways of communicating notice. It doesn't give any specific directives on the visual design of the platforms. Guidelines on following the Bill and considering the well-being of the data principal should thus be formulated by the design community.

The concern of accessibility and literacy is also not addressed by the Bill. It does mention issuing notices in multiple languages "where necessary and practical". Although all platforms are also supposed to follow accessibility guidelines issued by the government, there are no explicit recommendations in the Bill on how notices should be designed for accessibility. The design of platforms and notices specifically should have options for the persons with disabilities in the form of audio prompts. Visual notices would make them accessible to audiences who cannot read, or speak a certain language.